



Europäisches
Patentamt

Europäische
Patent Office

Office européen
des brevets

Bescheinigung

Certificate

Attestation

Die angehefteten Unterlagen stimmen mit der ursprünglich eingereichten Fassung der auf dem nächsten Blatt bezeichneten europäischen Patentanmeldung überein.

The attached documents are exact copies of the European patent application described on the following page, as originally filed.

Les documents fixés à cette attestation sont conformes à la version initialement déposée de la demande de brevet européen spécifiée à la page suivante.

Patentanmeldung Nr. Patent application No. Demande de brevet n°

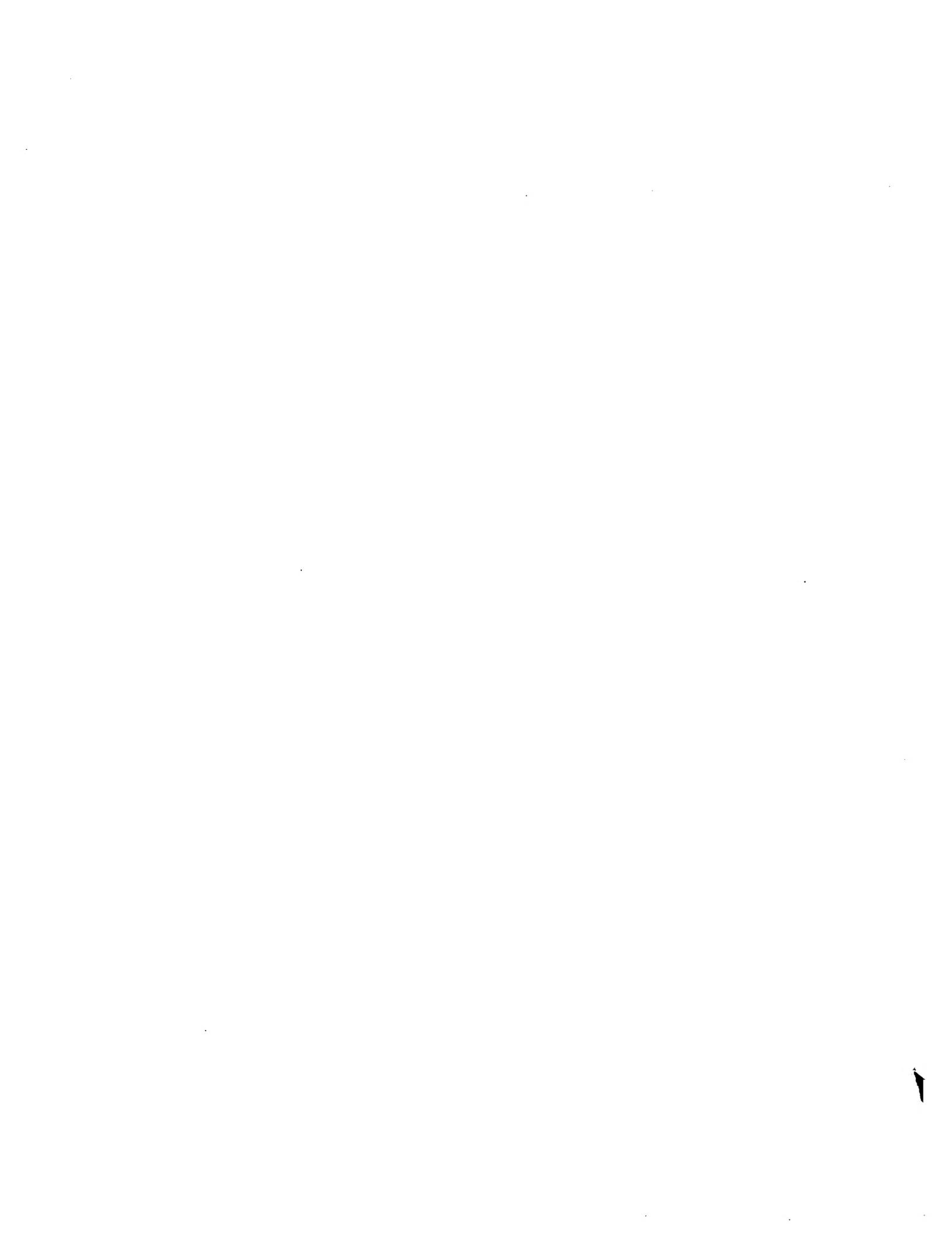
02102795.8

Der Präsident des Europäischen Patentamts;
Im Auftrag

For the President of the European Patent Office

Le Président de l'Office européen des brevets
p.o.

R C van Dijk





Anmeldung Nr:
Application no.: 02102795.8
Demande no:

Anmelde tag:
Date of filing: 18.12.02
Date de dépôt:

Anmelder/Applicant(s)/Demandeur(s):

International Business Machines Corporation
Armonk, NY 10504
UNITED STATES OF AMERICA

Bezeichnung der Erfindung/Title of the invention/Titre de l'invention:
(Falls die Bezeichnung der Erfindung nicht angegeben ist, siehe Beschreibung.
If no title is shown please refer to the description.
Si aucun titre n'est indiqué se référer à la description.)

Method of entering an authorization code into a chip card terminal

In Anspruch genommene Priorität(en) / Priority(ies) claimed /Priorité(s) revendiquée(s)

Staat/Tag/Aktenzeichen/State/Date/File no./Pays/Date/Numéro de dépôt:

Internationale Patentklassifikation/International Patent Classification/
Classification internationale des brevets:

G07F/

Am Anmelde tag benannte Vertragstaaten/Contracting states designated at date of filing/Etats contractants désignées lors du dépôt:

AT BE BG CH CY CZ DE DK EE ES FI FR GB GR IE IT LI LU MC NL
PT SE SI SK TR

D E S C R I P T I O N

**Method of entering an authorization code
into a chip card terminal**

Field of the invention

The present invention relates to the field of chip cards, which are also referred to as smart cards, data cards or integrated circuit cards, and more particularly, to chip card authentication.

Background and prior art

The use of chip cards is wide spread for a variety of applications, including electronic payment, electronic cash and access control systems. Typically a user has to insert the chip card into a terminal having a card reader. In order to enable a desired transaction the user has to input an authorization code into a keyboard of the terminal.

When the user has entered a valid authorization code the transaction is enabled. For example, payments at gas stations or other points of sales are usually performed this way by means of a credit card having an integrated circuit chip. The typical method for authenticating the user to the card by means of an authorization code involves the input of an personal identification number (PIN) into the terminal. The PIN is verified by means of the chip card. This verification is done by comparing the PIN with a reference PIN stored in a secret area of the non-volatile memory of the chip card.

This usual procedure of using smart cards for providing payments at points of sale has several security risks. One risk is that the user inputs his or her PIN information through the keyboard of the terminal which is owned by a third party. The keyboard can be tampered by the third party to read the user PIN number.

Another risk is that the terminals are typically located in public areas with no or only limited confidentiality. When the user enters his or her PIN number by means of the keyboard of the chip card terminal this can be easily observed by other customers. Especially this situation can occur when customers are queuing up in front of a point of sale.

Another disadvantage of entering the PIN number into the keyboard of the chip card terminal is that users frequently make mistakes when entering the PIN number or have forgotten the correct PIN number. This requires re-entering of the PIN number such that an extended period of time for the payment transaction is required. This is especially annoying for other customers who are standing in line in front of a crowded points of sale, such as in a gas station or supermarket.

The present invention therefore aims to provide an improved method of entering an authorization code into a chip card terminal and a corresponding computer program and chip card.

Summary of the invention

The present invention provides for an improved method of entering an authorization code into a chip card terminal whereby the authorization code is not directly entered into the chip card terminal but into the chip card itself. The authorization code is stored in a memory location of the chip card for a predetermined period of time.

During that period of time the authorization code can be transmitted from the memory location of the chip card to a chip card terminal. After the predefined period of time or after transmission of the authorization code the authorization code is erased from the memory location.

In accordance with a preferred embodiment of the invention the authorization code is an authentication code, such as a PIN number. For access control applications, such as access control

of buildings or other sites with restricted access, the authorization code can be a secret access code for authorizing access to the access-restricted site. Alternatively or in addition other data can be entered for transmission to the chip card terminal, such as a transaction number (TAN), a payment amount and/or a payment code indicating the purpose of the payment.

For example at a gas station the user can enter the number of the gasoline pump in addition to the PIN. The number of the gasoline pump is transmitted to the chip card terminal in addition to the PIN. This way it can be prevented that the wrong payment amount is deducted for another gasoline pump which the user has not used to fuel his or her car.

In accordance with a further preferred embodiment of the invention an aural, visual and/or haptic signal is outputted when the authorization code has been successfully entered into the chip card. For example the authorization code is verified by the chip card by means of reference verification data stored in a secured area of the memory of the chip card.

After successful verification the output signal is generated in order to inform the user that he or she entered a valid authorization code and that the chip card is in a state enabling the transmission of the previously entered authorization code to a chip card terminal. This way it can be prevented that the user has to re-enter his or her authorization code at the point of sale when a number of other users are waiting in line behind the user.

In accordance with a further preferred embodiment of the invention the signal is switched off after a predefined period of time or after the transmission of the authorization code to the chip card terminal has been successfully completed, whatever occurs earlier.

In accordance with a further preferred embodiment of the invention the user needs to continuously perform a predefined input action to maintain the enabling state of the chip card. For example, the user has to place his or her digit on a sensor element on the chip card, such as a photo element. When the user removes his or her finger from that sensor the chip card is reset and the transmission of the authorisation code to chip card terminal is disabled. This way misuse of the chip card after the authorization code has been entered is prevented.

In accordance to another preferred embodiment of the invention a bending or flexural sensor or switch is provided to detect an unsecure situation. For example if an attacker tries to take away the chip card from the user by physical force the chip card will undergo an elastic deformation which is sensed such that the authorization code is erased from the memory location of the chip card.

In accordance with a further preferred embodiment of the invention various elements of the user interface are not integrated into the chip card itself but in an electronic wallet. The electronic wallet has a slot for inserting the chip card in order to connect the chip card to the various external interface units. For example the electronic wallet can have a keyboard and a display which are connected to the chip card when the chip card is inserted in the electronic wallet.

In accordance with a further preferred embodiment of the invention the chip card is also used for service functions such as changing a PIN. The new PIN is entered into the chip card by means of the keyboard of the chip card or through the electronic wallet and confirmed.

It is to be noted that the present invention is particularly advantageous for making the usage of chip cards more secure and convenient. In particular the present invention provides for

improved protection of the confidentiality of the authorization code.

Another advantage is that the transaction time for providing a payment at a points of sale is reduced as manually entering the authorization code in the chip card terminal at the points of sale and re-entering of a previously incorrectly entered authorization code can be prevented.

Brief description of the drawings

In the following preferred embodiments of the invention will be described in greater detail by making reference to the drawings in which:

Figure 1 is a block diagram of an embodiment of a chip card,

Figure 2 is illustrative of a flow chart for performing a method of the invention.

Detailed description

Figure 1 schematically shows a chip card 100. Chip card 100 has a user interface 102. User interface 102 can comprise various elements, such as a keyboard, a display unit, a speaker, a light emitting diode and/or other input and output devices for providing an interface to the user. All of the elements of the user interface 102 can be integrated into chip card 100.

Alternatively some or all of the elements of user interface 102 can be provided by an electronic wallet. In this instance chip card 100 needs to be inserted into the electronic wallet in order to couple the chip card 100 to the respective user interface devices.

Further chip card 100 has a microprocessor 104 which is or can be coupled to user interface 102. Microprocessor 104 is coupled to memory 106 of chip card 100. Memory 106 has non-volatile, secret memory location 108 for storage of secret data. For

example a reference authorization code is stored in memory location 108. For improved protection of the reference authorization code it is preferred that the reference authorization code is encrypted.

Chip card 100 has state register 110 which is coupled to microprocessor 104. State register 110 serves to store state information which indicates whether chip card 100 is enabled to transmit the authorization code to a chip card terminal.

Further chip card 100 has terminal interface 112. Terminal interface 112 serves to couple chip card 100 to an external chip card terminal.

In operation a user of the chip card 100 inputs an authorization code, such as a PIN number, via user interface 102. From user interface 102 the authorization code 114, which has been inputted by the user, is provided to processor 104 which stores authorization code 114 in memory location 116 of memory 106.

Next processor 104 reads verification data 118 from the secret memory location 108. For example verification data 118 contains an encrypted reference authorization code. Processor 104 decrypts the reference authorization code contained in verification data 118 and compares reference authorization code and authorization code 114. If both codes are the same authorization is completed.

In response the processor 104 writes a status bit to state register 110. The status bit indicates that transmission of the authorization code 114 from memory location 116 to an external chip card terminal is enabled. Further processor 104 starts a timer. Preferably processor 104 provides an output signal to user interface 102 in order to inform the user that the entered authorization code 114 is correct and that the transmission of the authorization code 114 is enabled.

When the chip card 100 is subsequently inserted into the card reader of a chip card terminal this is signalled to processor 104 from the terminal interface 112 by means of signal 120 indicating the connection to the external chip card terminal. Next processor 104 checks the state register 110 and the timer. When the status bit is set in state register 110 and the timer is not expired processor 104 reads authorization code 114 from memory location 116 and transmits authorization code 114 via terminal interface 112 to the chip card terminal.

As a consequence the user does not need to enter authorization code 114 directly into the chip card terminal. This way the protection of the confidentiality of the authorization code 114 is improved. Another advantage is that other users who wait at a point of sale do not have to wait until user of chip card 100 has correctly entered his or her authorization code as the user can enter his or her authorization code 114 while standing in line in front of the point of sales check out terminal.

After transmission of the authorization code 114 or after the timer is expired, the state register 110 is reset. Preferably the processor 104 generates a corresponding output signal for user interface 102 in order to inform the user that the transmission is disabled now. Further the authorization code is erased from memory location 116.

As an alternative to the above described procedure an authorization signal is outputted from the chip card 100 to the external chip card terminal rather than the authorization code 114 itself. The authorization signal indicates to the external chip card terminal that the correct authorization code has been entered into the card and that authorization is complete. This has the additional advantage that when the card is stolen after entering the authorization code 114 the authorization code 114 is not outputted by the chip card.

Figure 2 illustrates a corresponding flow chart. In step 200 the user enters his or her authorization code into the chip card. In step 202 the authorization code is stored in an unsecure portion of the memory of the chip card. In step 204 the chip card verifies the authorization code by means of secret verification data which is stored in a secure memory location which is only accessible by the processor of the chip card.

If the verification (step 206) is not successful, i.e. the authorization card is not correct, a corresponding output message is provided to the user in step 208 and the user is prompted to re-enter its authorization code in step 200.

In case of successful verification the chip card changes its state in step 210 to enable the transmission of the authorization code to an external chip card terminal. For this purpose a corresponding output message is generated by the chip card such that the user is informed that the chip card is an enabled state.

If a terminal connection is established (step 214) the authorization code is transmitted to the external chip card terminal in step 216 and the chip card resets its state in step 218.

If no terminal connection is detected in step 214 the control goes to step 220. If the timer has not expired yet the control goes back to step 214 in order to check again whether a terminal connection has been established or not.

If it is determined in step 220 that the timer has expired in the meanwhile the control goes to step 218 in order to reset the state of the chip card in order to disable the transmission of the authorization code to the external chip card terminal.

In step 222 the authorization code in the non-secure memory location is erased by the chip card; this is necessary in order to ensure that the chip card is not misused if it gets into the

possession of an unauthorised user. Further the output of the message 'transmission enabled' via the user interface of the chip card is discontinued in step 224. Instead the message 'transmission disabled' is displayed.

L I S T O F R E F E R E N C E N U M E R A L S

100 Chip card
102 user interface
104 microprocessor
106 memory
108 memory locator
110 state register
112 terminal interface
114 authorization code
116 memory location
118 verification data
120 signal

6. The method of any one of the preceding claims 1 to 5, further comprising maintaining the second state only if a user continuously performs a predetermined input action during the predefined period of time.
7. The method of any one of the preceding claims 1 to 6, further comprising the steps of:
 - entering of an amount and/or a transaction code into the chip card,
 - transmitting of the amount and/or the code to the terminal when the authorization code is transmitted to the terminal.
8. The method of any one of the preceding claims 1 to 7, further comprising erasing the authorization code from the memory location if an unsecure situation is detected during the predefined period of time.
9. A chip card for enabling a transaction, the chip card comprising:
 - means (102) for entering of an authorization code (114),
 - means (104, 106, 116) for storing of the authorization code on the chip card,
 - means (104, 110) for changing a state of the chip card from a first state to a second state to enable transmission of the authorization code to a chip card terminal when the chip card is coupled to the chip card terminal within a pre-defined period of time and for resetting the state from the second to the first state.

C L A I M S

1. A method of entering an authorization code into a chip card terminal, the method comprising the steps of:
 - entering of the authorization code into a chip card,
 - storing of the authorization code in a memory location of the chip card,
 - changing a state of the chip card from a first state to a second state to enable transmission of the authorization code from the memory location to the chip card terminal when the chip card is coupled to the chip card terminal within a pre-defined period of time and resetting the state from the second to the first state.
2. The method of claim 1, further comprising verification of the authorization code and changing the state of the chip card from the first state to the second state only in case of a successful verification of the authorization code.
3. The method of claim 1 or 2, whereby the authorization code is an authentication code, a personal identification number (PIN) and/or transaction number (TAN) and/or an access code.
4. The method of claim 1, 2 or 3, whereby an aural, visual and/or haptic signal is outputted when the state is changed from the first state to the second state.
5. The method of claim 4, whereby the signal is switched off after the predefined period of time or after transmission of the authorization code to the terminal.

10. The chip card of claim 9 further comprising means (104; 108) for verification of the authorization code.
11. The chip card of claims 9 or 10, further comprising means (102) for outputting an aural, visual and/or haptic signal is outputted when the state is changed from the first state to the second state.
12. The chip card of claim 11, further comprising means (104) for switching off the signal after the predetermined period of time.
13. The chip card of any one of the preceding claims 9 to 12, further comprising means (102, 104) for maintaining the second state only if a user continuously performs a predetermined input action during the predefined period of time.
14. The chip card of any one of the preceding claims 9 to 13, further comprising means (102, 104) for detecting an unsecure situation and erasing the authorization code from the memory location, if an unsecure situation is detected.
15. The chip card of claim 14, the means for detecting an unsecure situation comprising a bending or flexural sensor or switch.
16. A computer program product, in particular digital storage medium, for entering of an authorization code into a chip card terminal, comprising program means for performing the steps of:
 - entering of the authorization code into a chip card,
 - storing of the authorization code in a memory location of the chip card,

- changing a state of the chip card from a first state to a second state to enable transmission of the authorization code from the memory location to the chip card terminal when the chip card is coupled to the chip card terminal within a pre-defined period of time and resetting the state from the second to the first state.

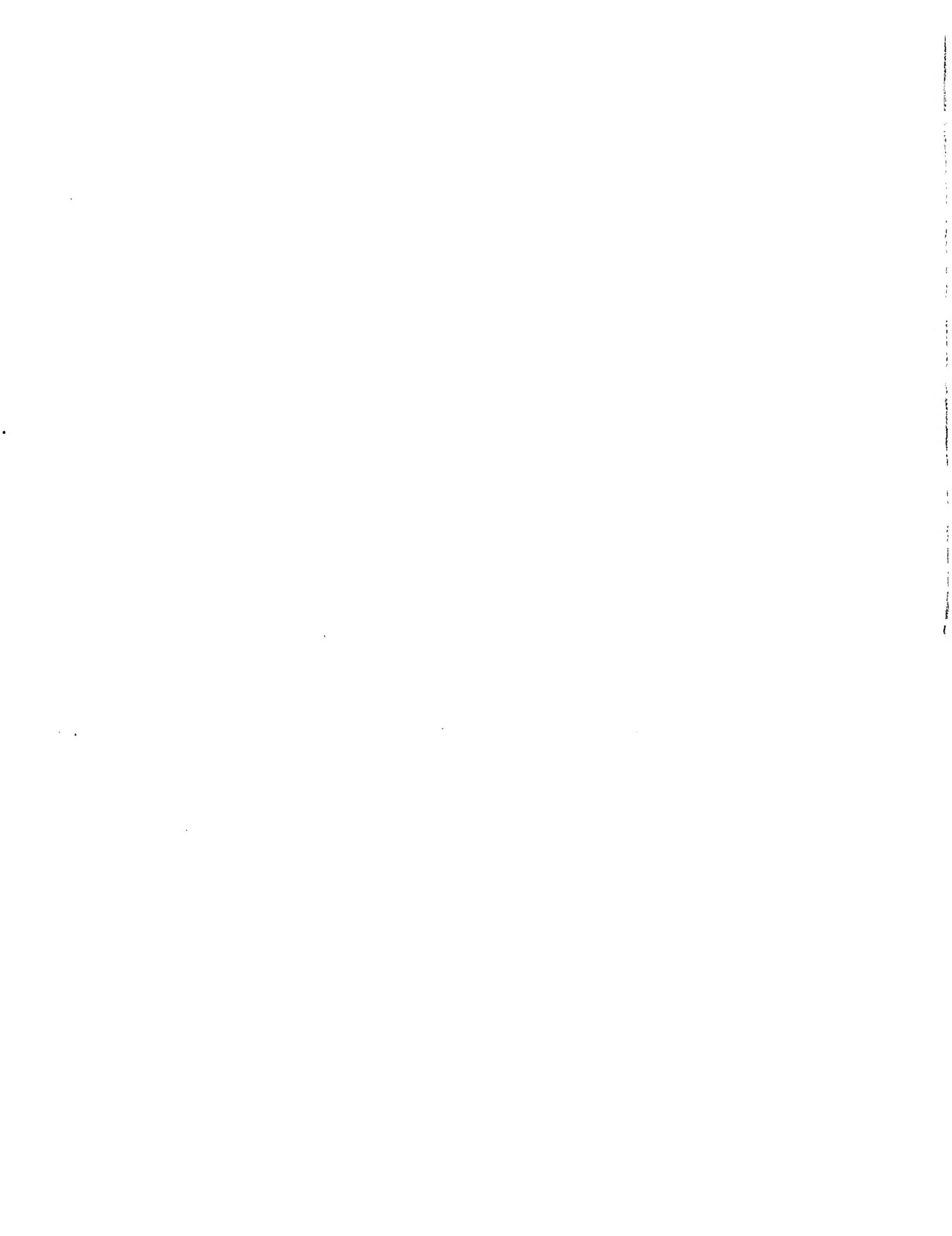
A B S T R A C T

Method of entering an authorization code into a chip card terminal

The invention relates to a method of entering an authorization code into a chip card terminal, the method comprising the steps of:

- entering of the authorization code into a chip card,
- storing of the authorization code in a memory location of the chip card,
- changing a state of the chip card from a first state to a second state to enable transmission of the authorization code from the memory location to the chip card terminal when the chip card is coupled to the chip card terminal within a pre-defined period of time and resetting the state from the second to the first state.

(Fig. 2)



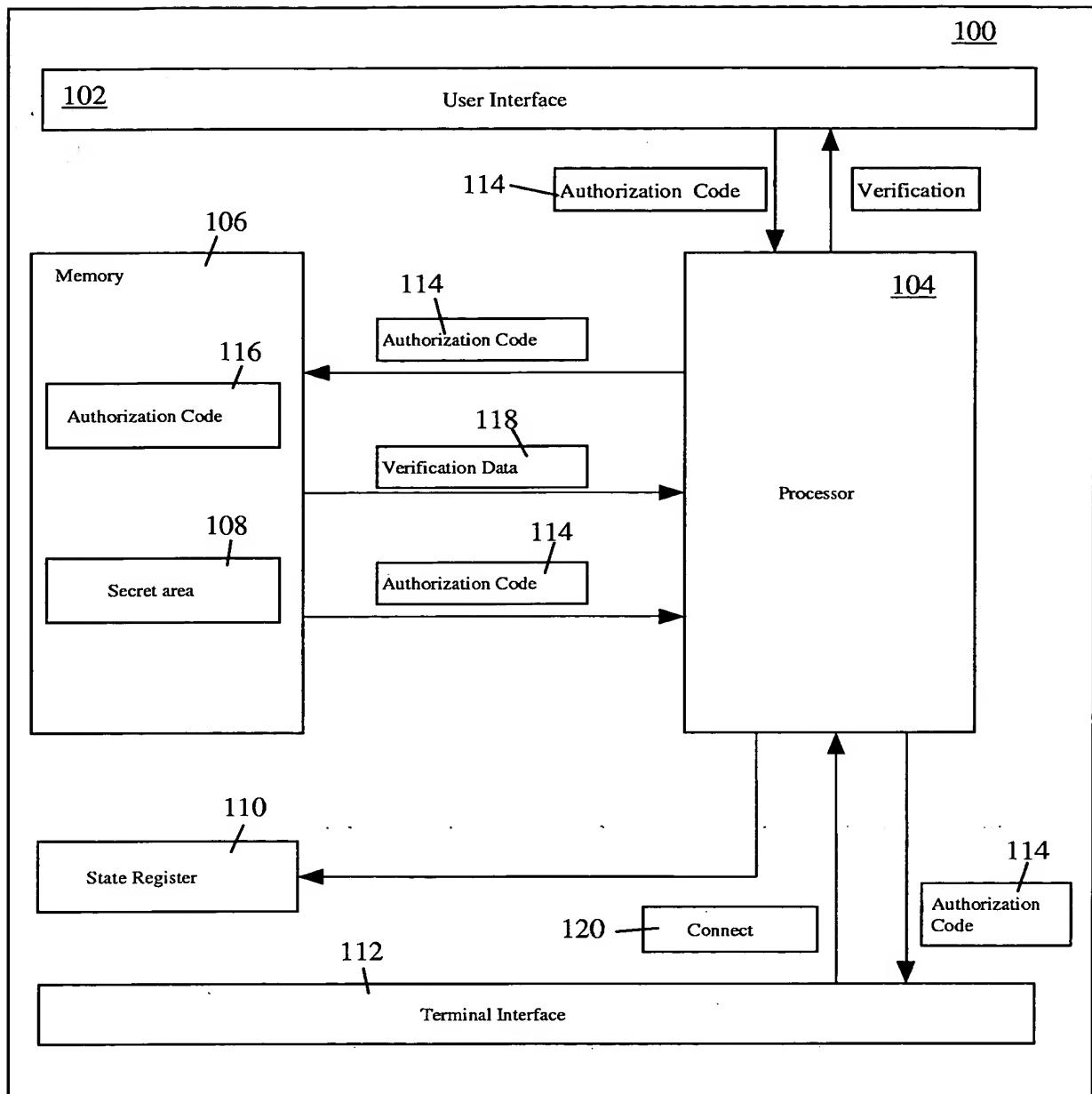


FIG. 1

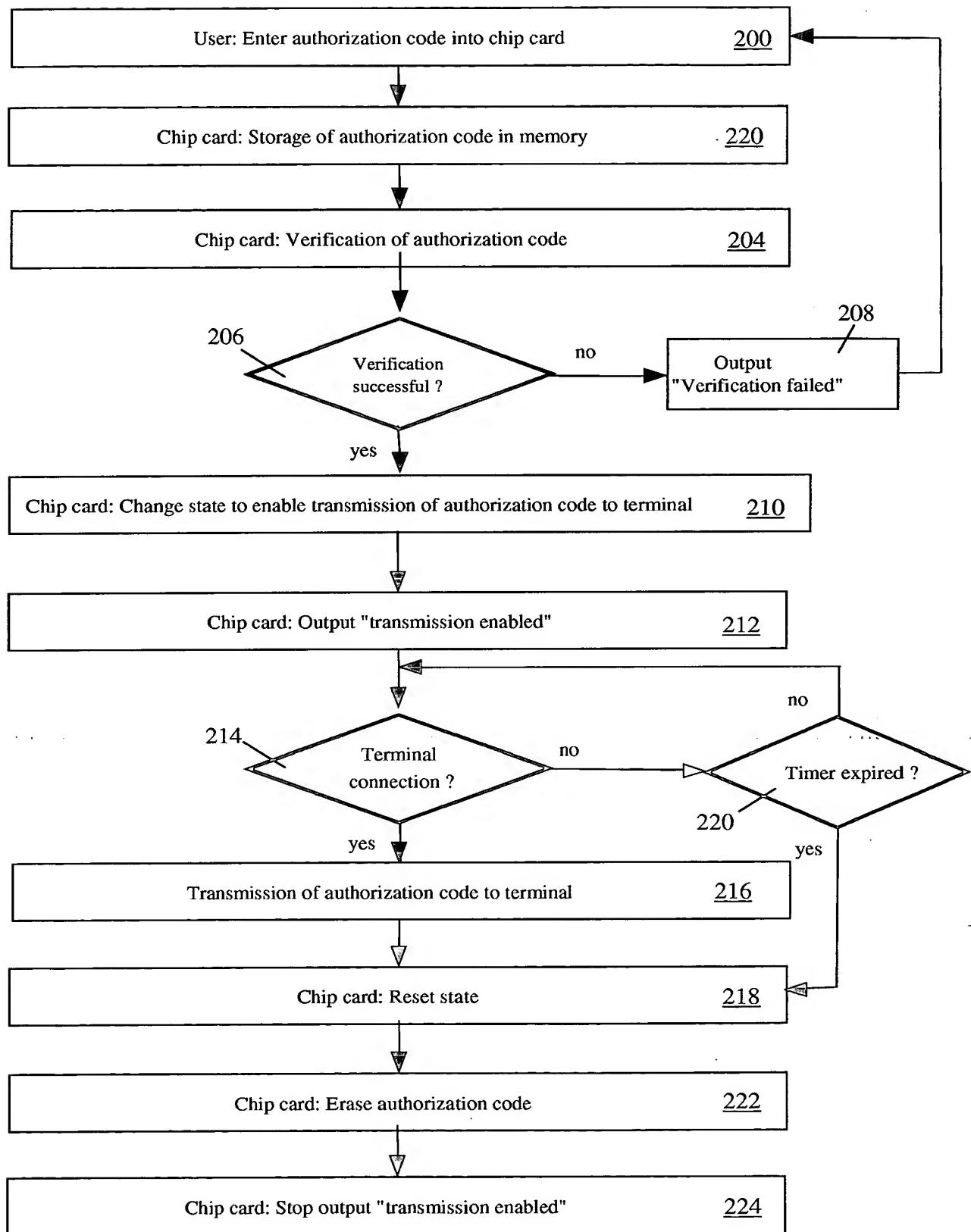


FIG. 2